

Biometrie

Technische Aspekte
Security-Überlegungen
Gesellschaftliche Aspekte
Lösungsansätze

cm@quintessenz.org

<http://www.quintessenz.org/>

Chaos Control 2003

Wien, 21. 5. 2003

Technisch

- Fehlerraten
 - zB Fingerabdruck: theoretisch 1:1Mio
 - Praktisch (Gesamtsystem): 1-5%
(= 4-20 auf eine Boeing 747)
- Fälschungsmöglichkeiten
 - Fachpresse, Unis: Fingerprint, Gesichtserkennung leicht überlistbar

Security-Überlegungen

- Viele Biometrische Merkmale sind nicht geheim
 - daher "stehlbar", vom Original oder aus dem System
- Something you know, something you have, something you are
 - Passworte abhören, Tokens stehlen, Biometrische Merkmale entführen?
- Wie umgehen mit "Identity Theft"?
 - Neues Paßwort, neues Token, neuer Körper?
- Wie mit vorgetäuschem "Identity Theft"?

Security-Überlegungen

- Auf welcher Grundlage wird ID mit Biometrie verknüpft?
- Drang zur Biometrie, statt organisatorische Probleme zu lösen?
- Problem des Insider-Mißbrauchs nicht gelöst
- Identifikation vs Verifikation

Gesellschaftlich

- Anonymität, Pseudonymität wird eingeengt
- Technikgläubigkeit: vgl Deutsche EC-Karten-
"Sicherheit"
- Überprüfbarkeit technischer Lösungen:
Vertrauen? Wem?

Lösungsansätze

- Zuerst das zu lösende Problem analysieren
- In abgeschlossenen Systemen
- Einverständnis der "Teilnehmer", Opt-Out?
- Smartcard mit Biometrie
- "Blacklisting": jeder darf, außer ...